#3

jc997 U.S. PTO
10/091003
03/06/02

Docket No. 220377US2S

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Yoshihisa ARAI

GAU:

SERIAL NO: NEW APPLICATION

EXAMINER:

FILED: Herewith

FOR: RANDOM NUMBER'S SEED GENERATING CIRCUIT, DRIVER HAVING THE SAME, AND SD MEMORY CARD SYSTEM

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date of U.S. Provisional Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §119(e)**.

☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
Japan	2001-063988	March 7, 2001

Certified copies of the corresponding Convention Application(s)

☒ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Marvin J. Spivak
Registration No. 24,913

C. Irvin McClelland
Registration Number 21,124

22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)

CIS/576-1

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年 ３月 ７日

出願番号
Application Number: 特願２００１－０６３９８８

出願人
Applicant(s): 株式会社東芝

２００１年１２月１４日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

【書類名】　特許願
【整理番号】　A000007586
【提出日】　平成13年 3月 7日
【あて先】　特許庁長官　殿
【国際特許分類】　G11C 7/00
【発明の名称】　乱数シード生成回路及びこれを備えたドライバ、並びに、ＳＤメモリカードシステム
【請求項の数】　18
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝マイクロエレクトロニクスセンター内
【氏名】　新居　欣久
【特許出願人】
【識別番号】　000003078
【氏名又は名称】　株式会社　東芝
【代理人】
【識別番号】　100058479
【弁理士】
【氏名又は名称】　鈴江　武彦
【電話番号】　03-3502-3181
【選任した代理人】
【識別番号】　100084618
【弁理士】
【氏名又は名称】　村松　貞男
【選任した代理人】
【識別番号】　100068814
【弁理士】
【氏名又は名称】　坪井　淳

出証特２００１－３１０８９０７

【選任した代理人】
【識別番号】　100092196
【弁理士】
【氏名又は名称】　橋本　良郎
【選任した代理人】
【識別番号】　100091351
【弁理士】
【氏名又は名称】　河野　哲
【選任した代理人】
【識別番号】　100088683
【弁理士】
【氏名又は名称】　中村　誠
【選任した代理人】
【識別番号】　100070437
【弁理士】
【氏名又は名称】　河井　将次
【手数料の表示】
【予納台帳番号】　011567
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　乱数シード生成回路及びこれを備えたドライバ、並びに、ＳＤメモリカードシステム

【特許請求の範囲】

【請求項１】　クロックを生成する発振器と、前記クロックに同期して動作するカウンタとを具備し、前記カウンタのカウント値は、前記クロックと非同期の信号に応答して出力され、その出力された前記カウント値が乱数を作成するための初期値として使用されることを特徴とする乱数シード生成回路。

【請求項２】　クロックを生成する発振器と、前記クロックに同期して動作するカウンタとを具備し、前記カウンタのカウント値を出力するタイミングは、信号に応答して一定範囲内でランダムに変化し、その出力された前記カウント値が乱数を作成するための初期値として使用されることを特徴とする乱数シード生成回路。

【請求項３】　前記信号は、電源が投入され、電源電位が安定したことを検知したパワーオンリセット回路から出力される信号であることを特徴とする請求項１又は２記載の乱数シード生成回路。

【請求項４】　前記信号は、コントローラから出力される動作開始信号であることを特徴とする請求項１又は２記載の乱数シード生成回路。

【請求項５】　前記動作開始信号は、電源が投入されたことを前記コントローラが認識したときに出力されることを特徴とする請求項４記載の乱数シード生成回路。

【請求項６】　前記動作開始信号は、機器利用者による所定の操作が行われたことを前記コントローラが認識したときに出力されることを特徴とする請求項４記載の乱数シード生成回路。

【請求項７】　前記発振器は、前記信号に応答して前記カウント値が出力された後に、非動作状態又は前記クロックの周波数を低くした状態となることを特徴とする請求項１又は２記載の乱数シード生成回路。

【請求項８】　前記発振器は、外部端子を持つ電圧制御可能な発振器であり、前記カウント値が出力される前は、前記外部端子と前記発振器が電気的に切断

出証特２００１－３１０８９０７

され、前記カウント値が出力された後は、前記外部端子と前記発振器が電気的に接続されることを特徴とする請求項１又は２記載の乱数シード生成回路。

【請求項９】　前記発振器と前記外部端子の間には、前記信号により制御されるスイッチ回路が接続されることを特徴とする請求項８記載の乱数シード生成回路。

【請求項１０】　前記カウント値が出力された後は、前記クロックは、システムクロックとして使用されることを特徴とする請求項８記載の乱数シード生成回路。

【請求項１１】　前記カウント値を出力するタイミングは、前記カウント値を出力する度に、前記クロックの周期よりも長い時間の範囲内で変化することを特徴とする請求項１又は２記載の乱数シード生成回路。

【請求項１２】　前記信号に基づいて前記カウント値をラッチするラッチ回路をさらに具備し、前記ラッチ回路にラッチされた前記カウント値が前記初期値として使用されることを特徴とする請求項１又は２記載の乱数シード生成回路。

【請求項１３】　前記信号が入力される乱数生成回路が動作状態となると同時に、前記カウント値が前記初期値として前記乱数生成回路に取り込まれることを特徴とする請求項１又は２記載の乱数シード生成回路。

【請求項１４】　クロックを生成する発振器及び前記クロックに同期して動作するカウンタを有する乱数シード生成回路と、前記乱数シード生成回路により生成された初期値を用いて乱数を生成する乱数生成回路とを具備し、前記カウンタのカウント値は、前記クロックと非同期の信号に応答して出力され、その出力された前記カウント値が前記初期値として使用され、前記乱数を用いて転送データの秘匿を行うことを特徴とするドライバ。

【請求項１５】　クロックを生成する発振器及び前記クロックに同期して動作するカウンタを有する乱数シード生成回路と、前記乱数シード生成回路により生成された初期値を用いて乱数を生成する乱数生成回路とを具備し、前記カウンタのカウント値を出力するタイミングは、信号に応答して一定範囲内でランダムに変化し、その出力された前記カウント値が前記初期値として使用され、前記乱数を用いて転送データの秘匿を行うことを特徴とするドライバ。

【請求項１６】　前記乱数は、電源が投入される度、前記データの書き込み若しくは読み出しを行う度、又は、機器利用者による所定の操作が行われる度に、作成されることを特徴とする請求項１４又は１５記載のドライバ。

【請求項１７】　クロックを生成する発振器及び前記クロックに同期して動作するカウンタを有する乱数シード生成回路と、前記乱数シード生成回路により生成された初期値を用いて乱数を生成する乱数生成回路とから構成されるドライバと、

前記ドライバにより駆動されるデータ保護機能を有するＳＤメモリカードと

を具備し、

前記カウンタのカウント値は、前記クロックと非同期の信号に応答して出力され、その出力された前記カウント値が前記初期値として使用され、前記乱数を用いて転送データの秘匿を行うことを特徴とするＳＤメモリカードシステム。

【請求項１８】　クロックを生成する発振器及び前記クロックに同期して動作するカウンタを有する乱数シード生成回路と、前記乱数シード生成回路により生成された初期値を用いて乱数を生成する乱数生成回路とから構成されるドライバと、

前記ドライバにより駆動されるデータ保護機能を有するＳＤメモリカードと

を具備し、

前記カウンタのカウント値を出力するタイミングは、信号に応答して一定範囲内でランダムに変化し、その出力された前記カウント値が前記初期値として使用され、前記乱数を用いて転送データの秘匿を行うことを特徴とするＳＤメモリカードシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、乱数を生成するときの初期値（シード）を決める乱数シード生成回路に関し、特に、デジタル信号処理回路に使用される。

【０００２】

【従来の技術】

従来、デジタル信号処理回路などのＬＳＩに乱数生成回路が搭載される場合、この乱数生成回路は、シフトレジスタや演算器などから構成される。乱数を生成する手法としては、従来より多種多様な手法が提案されているが、乱数を生成する元となる初期値（シード）については、システムの特性などを考慮して決めなければならないため、難しい問題の一つとなっている。

【０００３】

例えば、乱数生成回路により生成される乱数が適当な周期で変化していればよい（初期値はどうでもよい）システムの場合には、乱数シード（乱数の種）、即ち、初期値が、乱数を生成する度に、同じ値又は高い確率でほぼ同じ値になっても問題はない。このようなシステムとしては、例えば、乱数を用いてホワイトノイズを発生させるデジタルオーディオシステムなどが考えられる。

【０００４】

しかし、乱数生成回路により生成される乱数が、適当な周期で変化するだけでなく、その初期値が起動の度に異なる値となることが必要なシステムの場合には、乱数シード、即ち、初期値を、乱数を生成する度に、異なる値に設定しなければならない。このようなシステムとしては、図１３に示すように、乱数を用いてセキュリティに関する処理を行うシステム、例えば、ＳＤメモリカード（ SD memory card ）とそのドライバ（プレーヤ）との間で転送データを暗号化して秘匿するシステムが考えられる。

【０００５】

【発明が解決しようとする課題】

上述のように、乱数生成回路により生成される乱数が、適当な周期で変化するだけでなく、その初期値が起動の度に異なる値となることが必要なシステムの場合には、乱数シード、即ち、乱数の生成の元となる初期値を、乱数を生成する度に、異なる値に設定しなければならない。

【０００６】

しかし、従来の乱数生成回路では、乱数シードを、毎回、異なる値に設定することが非常に難しくなっている。

【０００７】

例えば、乱数生成回路がシフトレジスタから構成される場合を考えると、図１４に示すように、通常、電源が投入される度（乱数を生成する度）に、パワーオンリセット回路１０により、乱数生成回路（シフトレジスタ）１１の値がリセットされる。つまり、乱数生成回路１１のリセット動作により、その初期値は、常に、同じ値となってしまう。

【０００８】

また、このような事態を回避するため、パワーオンリセット回路１０により乱数生成回路１１の値がリセットされないようにしても、乱数生成回路１１の初期値は、チップごとに、高い確率で、同じ値となってしまう。

【０００９】

そこで、例えば、図１５に示すように、ＬＳＩに不揮発性メモリ１２を搭載し、電源を切った後には、この不揮発性メモリ１２に乱数生成回路（シフトレジスタ）１１の値を保持し、かつ、次の電源投入時には、この不揮発性メモリ１２に記憶された値を初期値として用いる、という技術がある。

【００１０】

しかし、一般的に、ＬＳＩに不揮発性メモリを搭載すると、ＬＳＩの製造コストが増大する、という問題が発生する。また、ＬＳＩによっては、製造プロセス上の理由から、不揮発性メモリを搭載することが非常に困難な場合がある。

【００１１】

本発明は、上述の問題を解決するためになされたもので、その目的は、不揮発性メモリを必要とすることなく、かつ、簡易な構成により、乱数シード（乱数生成回路に与える初期値）を起動の度にランダムに異ならせることができる乱数シード生成回路を提案することにある。

【００１２】

【課題を解決するための手段】

(1)　本発明の乱数シード生成回路は、クロックを生成する発振器と、前記クロックに同期して動作するカウンタとを備え、前記カウンタのカウント値は、前記クロックと非同期の信号に応答して出力され、その出力された前記カウント値が乱数を作成するための初期値として使用される。

【００１３】

本発明の乱数シード生成回路は、クロックを生成する発振器と、前記クロックに同期して動作するカウンタとを備え、前記カウンタのカウント値を出力するタイミングは、信号に応じて一定範囲内でランダムに変化し、その出力された前記カウント値が乱数を作成するための初期値として使用される。

【００１４】

前記信号は、電源が投入され、電源電位が安定したことを検知したパワーオンリセット回路から出力される信号である。

【００１５】

前記信号は、コントローラから出力される動作開始信号である。前記動作開始信号は、例えば、電源が投入されたことを前記コントローラが認識したときに出力される信号、又は、機器利用者による所定の操作が行われたことを前記コントローラが認識したときに出力される信号である。

【００１６】

前記発振器は、前記信号に応答して前記カウント値が出力された後に、非動作状態又は前記クロックの周波数を低くした状態となる。

【００１７】

前記発振器は、外部端子を持つ電圧制御可能な発振器であり、前記カウント値が出力される前は、前記外部端子と前記発振器が電気的に切断され、前記カウント値が出力された後は、前記外部端子と前記発振器が電気的に接続される。

【００１８】

前記発振器と前記外部端子の間には、前記信号により制御されるスイッチ回路が接続される。

【００１９】

前記カウント値が出力された後は、前記クロックは、システムクロックとして使用される。

【００２０】

前記カウント値を出力するタイミングは、前記カウント値を出力する度に、前記クロックの周期よりも長い時間の範囲内で変化する。

【００２１】

前記信号に基づいて前記カウント値をラッチするラッチ回路をさらに備え、前記ラッチ回路にラッチされた前記カウント値が前記初期値として使用される。

【００２２】

前記信号が入力される乱数生成回路が動作状態となると同時に、前記カウント値が前記初期値として前記乱数生成回路に取り込まれる。

【００２３】

(2)　本発明のドライバは、クロックを生成する発振器及び前記クロックに同期して動作するカウンタを有する乱数シード生成回路と、前記乱数シード生成回路により生成された初期値を用いて乱数を生成する乱数生成回路とを備える。前記カウンタのカウント値は、前記クロックと非同期の信号に応答して出力され、その出力された前記カウント値が前記初期値として使用され、前記乱数を用いて転送データの秘匿が行われる。

【００２４】

本発明のドライバは、クロックを生成する発振器及び前記クロックに同期して動作するカウンタを有する乱数シード生成回路と、前記乱数シード生成回路により生成された初期値を用いて乱数を生成する乱数生成回路とを備える。前記カウンタのカウント値を出力するタイミングは、信号に応答して一定範囲内でランダムに変化し、その出力された前記カウント値が前記初期値として使用され、前記乱数を用いて転送データの秘匿が行われる。

【００２５】

前記乱数は、電源が投入される度、前記データの書き込み若しくは読み出しを行う度、又は、機器利用者による所定の操作が行われる度に、作成される。

【００２６】

(3)　本発明のＳＤメモリカードシステムは、クロックを生成する発振器及び前記クロックに同期して動作するカウンタを有する乱数シード生成回路と、前記乱数シード生成回路により生成された初期値を用いて乱数を生成する乱数生成回路とから構成されるドライバとを備える。さらに、本発明のＳＤメモリカードシステムは、前記ドライバにより駆動されるデータ保護機能を有するＳＤメモリカ

ードを備える。

【００２７】

前記カウンタのカウント値は、前記クロックと非同期の信号に応答して出力され、その出力された前記カウント値が前記初期値として使用され、前記乱数を用いて転送データの秘匿が行われる。

【００２８】

本発明のＳＤメモリカードシステムは、クロックを生成する発振器及び前記クロックに同期して動作するカウンタを有する乱数シード生成回路と、前記乱数シード生成回路により生成された初期値を用いて乱数を生成する乱数生成回路とから構成されるドライバとを備える。さらに、本発明のＳＤメモリカードシステムは、前記ドライバにより駆動されるデータ保護機能を有するＳＤメモリカードを備える。

【００２９】

前記カウンタのカウント値を出力するタイミングは、信号に応答して一定範囲内でランダムに変化し、その出力された前記カウント値が前記初期値として使用され、前記乱数を用いて転送データの秘匿が行われる。

【００３０】

【発明の実施の形態】

以下、図面を参照しながら、本発明の乱数シード生成回路について詳細に説明する。

【００３１】

本発明の乱数シード生成回路は、不揮発性メモリを用いることなく、かつ、簡易な構成により乱数シードをランダムに生成することができる点に特徴を有する。以下では、まず、乱数シードをランダムに生成するための実施の形態を説明し、その後、本発明の乱数シード生成回路を用いたシステムの一例（応用例）について説明する。

【００３２】

[第１実施の形態]

図１は、本発明の第１実施の形態に関わる乱数シード生成回路について示して

いる。

【００３３】

乱数生成回路１１は、乱数シード生成回路１３から出力される乱数シード（初期値）に基づいて乱数を生成する。

【００３４】

乱数シード生成回路１３は、電源投入直後からクロックを生成し始める発振器１４と、この発振器１４から出力されるクロックに基づいて、カウント値を、順次、増加（又は減少）していくカウンタ１５と、取り込み信号に基づいてカウンタ１５のカウント値を取り込むラッチ回路１６とから構成される。

【００３５】

発振器１４は、電源が投入されると直ちに自己発振し、各機能ブロックや各回路などに発振出力を供給しなければならない。各機能ブロックや各回路などを動作可能状態にするためである。言い換えれば、電源が投入されると、発振器１４が最も先に動作し始めなければならない。また、発振器１４は、周期が数ｎｓ（例えば、５ｎｓ程度）の高速クロックを生成する。

【００３６】

なお、ＬＳＩ（例えば、デジタル信号処理回路）内に、十分に高い周波数（例えば、２００メガＨｚ程度）のクロックを生成する発振器（例えば、リングオシレータ）が内蔵されている場合には、この発振器により生成したクロックをカウンタ１５に与えてもよい。

【００３７】

カウンタ１５は、このような高速クロックに基づいて動作するため、カウンタ１５から出力されるカウント値も高速に変化する。

【００３８】

一方、取り込み信号は、発振器１４により生成される高速クロックとは非同期であり、かつ、電源が投入されてから取り込み信号がラッチ回路１６に入力されるまでの時間は、一定の範囲（例えば、数μｓ～数百ｍｓ）内で変化しており、この範囲は、発振器１４により生成されるクロックの周期（数ｎｓ）に対して十分に広くなっている。

【００３９】

つまり、電源が投入されてから取り込み信号がラッチ回路１６に入力されるまでの時間は、数μｓ～数百ｍｓの範囲でランダムに変化する一方、カウント値は、この範囲内で、数ｎｓの単位で高速に変化しているため、ラッチ回路１６にラッチされるカウント値は、電源投入の度に、ランダムに変化することになる。

【００４０】

また、ラッチ回路１６にラッチされたカウント値は、乱数シード（初期値）となるため、結果として、乱数シードを、電源投入の度に、ランダムに変化させることができる。

【００４１】

なお、取り込み信号としては、例えば、パワーオンリセット回路１０の出力信号とすることができる。この場合、パワーオンリセット回路１０は、電源が投入され、かつ、ＬＳＩ内部で使用する電源が安定状態となった後に、パワーオンリセット信号（取り込み信号）を出力する。

【００４２】

ここで、パワーオンリセット信号は、発振器１４により生成されるクロックとは非同期であり、かつ、電源が投入されてからＬＳＩ内部で使用する電源が安定状態となるまでの時間は、通常、数μｓ～数百ｍｓであるため、パワーオンリセット回路１０の出力信号を取り込み信号として用いることは、本発明にとって好都合である。

【００４３】

このように、本実施の形態では、例えば、図２の波形図に示すように、電源が投入されてから取り込み信号がラッチ回路１６に入力されるまでの時間の範囲を、カウント値が変化する時間（クロックの周期）よりも十分に大きくしており、また、電源が投入されてから取り込み信号がラッチ回路１６に入力されるまでの時間は、この範囲内でランダムに変化するため、乱数シードを、電源投入の度に、ランダムに変化させることができる。

【００４４】

［第２実施の形態］

本実施の形態に関わる乱数シード生成回路は、上述の第１実施の形態に関わる乱数シード生成回路の変形例である。

【００４５】

本実施の形態の乱数シード生成回路は、上述の第１実施の形態に関わる乱数シード生成回路と比べると、①　カウント値をラッチするラッチ回路を省略し、②　パワーオンリセット回路の出力信号を、乱数生成回路の動作開始信号として、直接、乱数生成回路に入力した点に特徴を有する。

【００４６】

この場合、パワーオンリセット回路の出力信号（動作開始信号）は、従来のように、乱数シード（初期値）をリセットしない。即ち、本実施の形態では、パワーオンリセット回路の出力信号が乱数生成回路に入力された時点で、乱数シード生成回路内のカウンタのカウント値に基づいて乱数シードが決定され、かつ、乱数生成回路において乱数を生成する動作が開始する。

【００４７】

以下、本実施の形態に関わる乱数シード生成回路について詳細に説明する。

【００４８】

図３は、本発明の第２実施の形態に関わる乱数シード生成回路について示している。

【００４９】

乱数生成回路１１は、乱数シード生成回路１３から出力される乱数シード（初期値）に基づいて乱数を生成する。乱数シード生成回路１３は、電源投入直後からクロックを生成し始める発振器１４と、この発振器１４から出力されるクロックに基づいて、カウント値を、順次、増加（又は減少）していくカウンタ１５とから構成される。

【００５０】

発振器１４は、電源が投入されると直ちに自己発振し、各機能ブロックや各回路などに発振出力を供給しなければならない。各機能ブロックや各回路などを動作可能状態にするためである。言い換えれば、電源が投入されると、発振器１４が最も先に動作し始めなければならない。また、発振器１４は、周期が数ｎｓ（

例えば、５ｎｓ程度）の高速クロックを生成する。

【００５１】

なお、上述の第１実施の形態と同様に、ＬＳＩ内に設けられる別の発振器（例えば、リングオシレータ）を利用して、カウンタ１５に与えるクロックを生成してもよい。

【００５２】

カウンタ１５は、このような高速クロックに基づいて動作するため、カウンタ１５から出力されるカウント値も高速に変化する。

【００５３】

一方、動作開始信号は、発振器１４により生成される高速クロックとは非同期であり、かつ、電源が投入されてからＬＳＩ内部で使用する電源が安定状態となるまでの時間、具体的には、電源が投入された後、パワーオンリセット回路１０から動作開始信号が出力されるまでの時間は、一定の範囲（例えば、数μｓ～数百ｍｓ）内で変化しており、この範囲は、発振器１４により生成されるクロックの周期（数ｎｓ）に対して十分に広くなっている。

【００５４】

つまり、電源が投入されてから動作開始信号が乱数生成回路１１に入力されるまでの時間は、数μｓ～数百ｍｓの範囲でランダムに変化する一方、カウント値は、この範囲内で、数ｎｓの単位で高速に変化しているため、乱数生成回路１１が動作を開始するときの乱数シード（カウント値）は、電源投入の度に、ランダムに変化する。

【００５５】

このように、本実施の形態では、電源が投入されてから、動作開始信号が乱数生成回路１１に入力されるまでの時間の範囲を、カウント値が変化する時間（クロックの周期）よりも十分に大きくしている。このため、電源が投入されてから動作開始信号が乱数生成回路１１に入力されるまでの時間が、この範囲内でランダムに変化することにより、乱数シードを、電源投入の度に、ランダムに変化させることができる。

【００５６】

また、本実施の形態では、カウンタ１５のカウント値が、直接、乱数生成回路１１に入力される。そして、動作開始信号が乱数生成回路に入力された時点で、乱数シードが決定され、同時に、乱数生成回路において乱数を生成する動作が開始される。このため、乱数シード生成回路の面積縮小、設計容易化、製造コストの低下などの独自の効果を得ることができる。

【００５７】

[第３実施の形態]

図４は、本発明の第３実施の形態に関わる乱数シード生成回路について示している。

【００５８】

乱数生成回路１１は、乱数シード生成回路１３から出力される乱数シード（初期値）に基づいて乱数を生成する。

【００５９】

乱数シード生成回路１３は、電源投入直後からクロックを生成し始める発振器１４と、この発振器１４から出力されるクロックに基づいて、カウント値を、順次、増加（又は減少）していくカウンタ１５と、コントローラ２１からの動作開始信号（取り込み信号）に基づいてカウンタ１５のカウント値を取り込むラッチ回路１６とから構成される。

【００６０】

発振器１４は、電源が投入されると直ちに自己発振し、各機能ブロックや各回路などに発振出力を供給しなければならない。各機能ブロックや各回路などを動作可能状態にするためである。言い換えれば、電源が投入されると、発振器１４が最も先に動作し始めなければならない。また、発振器１４は、周期が数ｎｓ（例えば、５ｎｓ程度）の高速クロックを生成する。

【００６１】

なお、上述の第１実施の形態と同様に、ＬＳＩ内に設けられる別の発振器（例えば、リングオシレータ）を利用して、カウンタ１５に与えるクロックを生成してもよい。

【００６２】

カウンタ１５は、このような高速クロックに基づいて動作するため、カウンタ１５から出力されるカウント値も高速に変化する。

【００６３】

一方、カウンタ１５のカウント値をラッチ回路１６に取り込むタイミングは、コントローラ（ホストマイコン）２１からの動作開始信号により決定される。

【００６４】

コントローラ２１からの動作開始信号とは、何らかの処理を行うために乱数が必要になったときに、コントローラ２１が乱数生成回路１１を動作させるために出力する信号のことであり、発振器１４により生成されるクロックとは非同期である。

【００６５】

例えば、ＳＤカードを使ったシステム（図１２）では、システムコントロール用ＣＰＵ（コントローラ）２１、ＳＤカードインターフェイス回路２２や、その他のデジタル信号処理回路（ＤＳＰ）２３などを用いて、ＳＤカード２４にデータを書き込んだり、又は、ＳＤカード２４からデータを読み出したりする。

【００６６】

ここで、ＳＤカード２４に対してデータの書き込み又は読み出しを行う際には、システムコントロール用ＣＰＵ２１は、ＳＤカード２４へのアクセスを指示する信号を出力することになる。

【００６７】

そこで、このＳＤカード２４に対するアクセスを指示する信号を、動作開始信号としてラッチ回路１６に供給し、乱数シードの取り込みに利用する。

【００６８】

一般に、システムコントロール用ＣＰＵ２１の動作クロックは、ＳＤカードインターフェイス回路２２の動作を制御するクロックに対して非同期であり、さらに、システムコントロール用ＣＰＵ２１から出力される動作開始信号の周期は、数μｓ程度となっている。つまり、カウンタ１５の動作速度（カウント値が変化する速度）は、この動作開始信号の動作速度（周波数）よりも十分に速くなっているため、ラッチ回路１６にラッチされるカウント値は、動作開始信号が出力さ

れる度に、ランダムに変化することになる。

【００６９】

また、ラッチ回路１６にラッチされたカウント値は、乱数シード（初期値）となるため、結果として、乱数シードを、動作開始信号が出力される度に、ランダムに変化させることができる。

【００７０】

このように、本実施の形態では、システムコントローラ２１からの動作開始信号に基づいて、カウント値を取り込むタイミング、即ち、乱数シードを決定している。従って、乱数シードを、動作開始信号を出力する度に、ランダムに変化させることができる。

【００７１】

なお、本実施の形態においては、システムコントローラ２１からの動作開始信号を、機器利用者（又はシステム利用者）の操作によるタイミングとすることができる。例えば、ＳＤカードを使ったオーディオプレーヤであれば、機器利用者が再生ボタンを押したタイミングや、ＳＤカードをプレーヤ内に挿入したタイミングで、動作開始信号が出力されるようにしてもよい。

【００７２】

［第４実施の形態］

本実施の形態に関わる乱数シード生成回路は、上述の第３実施の形態に関わる乱数シード生成回路の変形例である。

【００７３】

本実施の形態の乱数シード生成回路は、上述の第３実施の形態の乱数シード生成回路と比べると、①　カウント値をラッチするラッチ回路を省略し、②　コントローラ２１からの動作開始信号を、直接、乱数生成回路に入力した点に特徴を有する。

【００７４】

この場合、コントローラ２１からの動作開始信号が乱数生成回路に入力された時点で、乱数シード生成回路内のカウンタのカウント値に基づいて乱数シードが決定され、かつ、乱数生成回路において乱数を生成する動作が開始する。

【００７５】

以下、本実施の形態に関わる乱数シード生成回路について詳細に説明する。

【００７６】

図５は、本発明の第４実施の形態に関わる乱数シード生成回路について示している。

【００７７】

乱数生成回路１１は、乱数シード生成回路１３から出力される乱数シード（初期値）に基づいて乱数を生成する。乱数シード生成回路１３は、電源投入直後からクロックを生成し始める発振器１４と、この発振器１４から出力されるクロックに基づいて、カウント値を、順次、増加（又は減少）していくカウンタ１５とから構成される。

【００７８】

発振器１４は、電源が投入されると直ちに自己発振し、各機能ブロックや各回路などに発振出力を供給しなければならない。各機能ブロックや各回路などを動作可能状態にするためである。言い換えれば、電源が投入されると、発振器１４が最も先に動作し始めなければならない。また、発振器１４は、周期が数ｎｓ（例えば、５ｎｓ程度）の高速クロックを生成する。

【００７９】

なお、上述の第１実施の形態と同様に、ＬＳＩ内に設けられる別の発振器（例えば、リングオシレータ）を利用して、カウンタ１５に与えるクロックを生成してもよい。

【００８０】

カウンタ１５は、このような高速クロックに基づいて動作するため、カウンタ１５から出力されるカウント値も高速に変化する。

【００８１】

一方、カウンタ１５のカウント値が乱数シードとして乱数生成回路１１に入力されるタイミングは、コントローラ（ホストマイコン）２１からの動作開始信号により決定される。

【００８２】

コントローラ２１からの動作開始信号とは、何らかの処理を行うために乱数が必要になったときに、コントローラ２１が乱数生成回路１１を動作させるために出力する信号のことであり、発振器１４により生成されるクロックとは非同期である。

【００８３】

なお、コントローラ２１から動作開始信号が出力されるタイミングとしては、機器利用者（又はシステム利用者）の操作によるタイミングを利用することができる。例えば、ＳＤカードを使ったオーディオプレーヤであれば、システム利用者が再生ボタンを押したタイミングや、ＳＤカードをシステム内に挿入したタイミングで、動作開始信号が出力されるようにしてもよい。

【００８４】

このように、本実施の形態では、コントローラ２１からの動作開始信号に基づいて、カウント値を取り込むタイミング、即ち、乱数シードを決定している。従って、乱数シードを、動作開始信号を出力する度に、ランダムに変化させることができる。

【００８５】

また、本実施の形態では、カウンタ１５のカウント値が、直接、乱数生成回路１１に入力され、動作開始信号に基づいて乱数シードが決定される。このため、乱数シード生成回路の面積縮小、設計容易化、製造コストの低下などの独自の効果を得ることができる。

【００８６】

［第５実施の形態］

本実施の形態に関わる乱数シード生成回路は、上述の第３実施の形態に関わる乱数シード生成回路の変形例である。

【００８７】

図６は、本発明の第５実施の形態に関わる乱数シード生成回路について示している。

【００８８】

本実施の形態の乱数シード生成回路１３は、上述の第３実施の形態の乱数シー

ド生成回路と比べると、コントローラ２１からの動作開始信号を、発振器１４の動作を停止させる発振停止信号として、発振器１４にも入力した点に特徴を有する。その他の構成については、上述の第３実施の形態に関わる乱数シード生成回路と全く同一である。

【００８９】

本発明の乱数シード生成回路１３では、乱数シード（初期値）が決定された後には、乱数シード生成回路１３を動作させておく必要がない。

【００９０】

そこで、本実施の形態では、コントローラ２１からの動作開始信号により、乱数シードをラッチ回路１６にラッチすると同時に、発振器１４の動作を停止させて、消費電力の削減を図っている。

【００９１】

なお、本実施の形態では、乱数シードが決定された後に、発振器１４を非動作状態にしたが、例えば、これに代えて、発振器１４により生成されるクロックの周波数を十分に低くしても、消費電力の削減を実現できる。

【００９２】

［第６実施の形態］

本実施の形態に関わる乱数シード生成回路は、上述の第４実施の形態に関わる乱数シード生成回路の変形例である。

【００９３】

図７は、本発明の第６実施の形態に関わる乱数シード生成回路について示している。

【００９４】

本実施の形態の乱数シード生成回路１３は、上述の第４実施の形態の乱数シード生成回路と比べると、コントローラ２１からの動作開始信号を、発振器１４の動作を停止させる発振停止信号として、発振器１４にも入力した点に特徴を有する。その他の構成については、上述の第４実施の形態に関わる乱数シード生成回路と全く同一である。

【００９５】

上述の第５実施の形態で説明したように、本発明の乱数シード生成回路では、コントローラ２１からの動作開始信号により、乱数シード（初期値）が決定された後には、乱数シード生成回路１３を動作させておく必要がない。

【００９６】

そこで、本実施の形態では、コントローラ２１からの動作開始信号により、乱数生成回路１１が動作し、乱数シードが決定されると同時に、発振器１４の動作を停止させて、消費電力の削減を図っている。

【００９７】

なお、本実施の形態においても、発振器１４に関しては、乱数生成回路１１を動作状態にした後には、発振周波数を十分に低くして、消費電力の削減を図ってもよい。

【００９８】

［第７実施の形態］

本実施の形態に関わる乱数シード生成回路は、悪意を持って本発明の集積回路を解析する、という行為を防止すべく、電源が投入されてから乱数シードの取り込みが完了するまでは、ＬＳＩの外部から乱数シード生成回路内の発振器を制御できないようにした点、及び、乱数シード生成回路内の発振器から出力されるクロックを、乱数を用いて動作するシステムの動作クロックとして使用した点に特徴を有する。

【００９９】

図８は、本発明の第７実施の形態に関わる乱数シード生成回路について示している。

【０１００】

乱数生成回路１１は、乱数シード生成回路１３から出力される乱数シード（初期値）に基づいて乱数を生成する。

【０１０１】

乱数シード生成回路１３は、電源投入直後からクロックを生成し始める電圧制御可能な発振器（ＶＣＯ： Voltage Controlled Oscillator ）１４Ａと、この発振器１４Ａから出力されるクロックに基づいて、カウント値を、順次、増加（

又は減少）していくカウンタ１５と、コントローラ２１からの動作開始信号（取り込み信号）に基づいてカウンタ１５のカウント値を取り込むラッチ回路１６とを有する。

【０１０２】

また、本実施の形態では、発振器１４Ａから出力されるクロックをシステム動作クロックとしても使用している。このため、乱数シード生成回路１３は、さらに、発振器１４Ａから出力されるクロックの周波数を一定値に安定させるためのＰＬＬ（ Phase Locked Loop ）回路を備えている。

【０１０３】

ＰＬＬ回路は、基準クロックの周波数を分周する分周器１７Ａと、発振器１４Ａから出力されるクロックを分周する分周器１７Ｂと、分周器１７Ａから出力されるクロックと分周器１７Ｂから出力されるクロックの位相を比較する位相比較器１８と、抵抗及びキャパシタからなるＬＰＦ（ローパスフィルタ）１９と、コントローラ２１からの動作開始信号により制御されるスイッチ回路２４とから構成される。

【０１０４】

発振器１４Ａは、電源が投入されると直ちに自己発振し、各機能ブロックや各回路などに発振出力を供給しなければならない。各機能ブロックや各回路などを動作可能状態にするためである。言い換えれば、電源が投入されると、発振器１４Ａが最も先に動作し始めなければならない。

【０１０５】

また、発振器１４Ａは、周期が数ｎｓ（例えば、５ｎｓ程度）の高速クロックを生成する。この時、スイッチ回路２４は、オフ状態となっており、ＰＬＬ回路は、機能していない。ＬＳＩの外部から発振器１４Ａの周波数を制御できないようにするためである。

【０１０６】

なお、カウンタ１５は、このような高速クロックに基づいて動作するため、カウンタ１５から出力されるカウント値も高速に変化する。

【０１０７】

一方、電源が投入されてから数μｓ～数百ｍｓが経過した後に、コントローラ２１からの動作開始信号がラッチ回路１６及びスイッチ回路２４に入力される。この範囲は、発振器１４Ａにより生成されるクロックの周期（数ｎｓ）に対して十分に広くなっており、また、動作開始信号は、発振器１４により生成されるクロックとは非同期である。

【０１０８】

つまり、電源が投入されてからコントローラ２１からの動作開始信号がラッチ回路１６に入力されるまでの時間は、数μｓ～数百ｍｓの範囲でランダムに変化する一方、カウント値は、この範囲内で、数ｎｓの単位で高速に変化するため、ラッチ回路１６にラッチされるカウント値は、電源投入の度に、ランダムに変化することになる。

【０１０９】

また、ラッチ回路１６にラッチされたカウント値は、乱数シード（初期値）となるため、結果として、乱数シードを、電源投入の度に、ランダムに変化させることができる。

【０１１０】

ところで、本実施の形態では、コントローラ２１からの動作開始信号がラッチ回路１６に入力され、乱数シードが決定されると同時に、スイッチ回路２４がオン状態となり、ＰＬＬ回路が機能し始める。そして、乱数シード生成回路１３内の発振器１４Ａから出力されるクロックを、乱数を用いて動作するシステムの動作クロックとしても使用する。

【０１１１】

例えば、図１２に示すようなシステムにおいては、インターフェイス回路２２を動作させるために、２０メガＨｚ程度の動作クロックが必要となるが、この動作クロックとして、図８の乱数シード生成回路１３内の発振器１４Ａから出力されるクロックを使用する。

【０１１２】

通常のＬＳＩでは、多くの場合、発振器（ＶＣＯ）から出力されるクロックの周波数を一定値に安定させるためには、ＰＬＬ回路による制御が必要となる。こ

こで、ＰＬＬ回路は、ＬＰＦ（ローパスフィルタ）１９を備えているが、このＬＰＦ１９は、ＬＳＩの外部に、いわゆる外付け部品として接続される。

【０１１３】

しかし、このことは、発振器（ＶＣＯ）から出力されるクロックの周波数（発振周波数）を、ＬＳＩの外部から制御できることを意味するため、乱数シードが自由にコントロールされ、悪意の解析者からデータを保護することができなくなる、という問題が生じる。

【０１１４】

即ち、外付け部品を取り除き、発振器（ＶＣＯ）１４Ａを制御する電圧を自由に制御できるようにすれば、例えば、発振器１４Ａの発振周波数を十分に低くして（カウンタ１５のカウント値がほとんど変わらないようにして）、電源投入の度に、乱数シードをほぼ同じ値又は全く同じ値にすることも可能である。

【０１１５】

そこで、本実施の形態では、電源が投入されてから乱数シードが決定されるまでは、スイッチ回路２４をオフ状態にし、発振器（ＶＣＯ）１４ＡがＰＬＬ回路（又はＬＳＩ外部の悪意の解析者）により制御されないようにしている。

【０１１６】

なお、コントローラ２１からの動作開始信号により、カウンタ値がラッチ回路１６に取り込まれ、かつ、乱数シードが決定された後には、スイッチ回路２４がオン状態となり、ＰＬＬ回路による発振器（ＶＣＯ）１４Ａの制御が開始される。

【０１１７】

スイッチ回路２４がオン状態になると、例えば、ＬＳＩの外部からの制御により、発振器１４Ａの発振周波数を極端に低く又は停止させることも可能になるが、本実施の形態では、発振器１４Ａから出力されるクロックをシステムの動作クロックとしても使用しているため、ＬＳＩの動作を解析される恐れはない。

【０１１８】

つまり、発振器１４Ａの発振周波数を極端に低く又は停止させると、システム自体が動作しなくなる。

【０１１９】

このように、本実施の形態では、第一に、電源が投入されてからコントローラ２１からの動作開始信号（取り込み信号）がラッチ回路１６に入力されるまでの時間の範囲を、カウント値が変化する時間（クロックの周期）よりも十分に大きくしており、また、電源が投入されてからこの動作開始信号がラッチ回路１６に入力されるまでの時間は、この範囲内でランダムに変化するため、乱数シードを、電源投入の度に、ランダムに変化させることができる。

【０１２０】

また、第二に、乱数シード生成回路内の発振器から出力されるクロックを、乱数を用いて動作するシステムの動作クロックとして使用し、かつ、ＰＬＬ回路により動作クロックの周波数の安定化を図った場合において、電源が投入されてから乱数シードの取り込みが完了するまでは、ＬＳＩの外部から乱数シード生成回路内の発振器を制御できないようにしているため、悪意を持った解析者からデータを保護することができる。

【０１２１】

［第８実施の形態］

図９は、本発明の第８実施の形態に関わる乱数シード生成回路について示している。

【０１２２】

本実施の形態に関わる乱数シード生成回路は、上述の第７実施の形態に関わる乱数シード生成回路の変形例である。

【０１２３】

本実施の形態の乱数シード生成回路は、上述の第７実施の形態に関わる乱数シード生成回路と比べると、①　カウント値をラッチするラッチ回路を省略し、②　コントローラ２１からの動作開始信号を、乱数生成回路１１の動作開始信号として、直接、乱数生成回路１１に入力した点に特徴を有する。

【０１２４】

この場合、コントローラ２１からの動作開始信号が乱数生成回路１１に入力された時点で、乱数シード生成回路１３内のカウンタ１５のカウント値に基づいて

乱数シードが決定され、かつ、乱数生成回路１１において乱数を生成する動作が開始する。

【０１２５】

このように、本実施の形態では、コントローラ２１からの動作開始信号に基づいて、カウント値を取り込むタイミング、即ち、乱数シードを決定している。従って、乱数シードを、動作開始信号を出力する度に、ランダムに変化させることができる。

【０１２６】

また、乱数シード生成回路内の発振器から出力されるクロックを、乱数を用いて動作するシステムの動作クロックとして使用し、電源が投入されてから乱数シードの取り込みが完了するまでは、ＬＳＩの外部から乱数シード生成回路内の発振器を制御できないようにしているため、悪意を持った解析者からデータを保護できる。

【０１２７】

さらに、本実施の形態では、カウンタ１５のカウント値が、直接、乱数生成回路１１に入力され、動作開始信号に基づいて乱数シードが決定される。このため、乱数シード生成回路の面積縮小、設計容易化、製造コストの低下などの独自の効果を得ることができる。

【０１２８】

［応用例］

以下、上述の第１乃至第８実施の形態に関わる乱数シード生成回路を、ＳＤメモリカード（ Secure Digital Memory Card ）を使ったシステムに適用した応用例について説明する。

【０１２９】

図１０及び図１１は、ＳＤメモリカードシステムの概要を示している。

【０１３０】

ＳＤメモリカードとは、強力な著作権保護機能を有する点を一つの特徴とするメモリカードのことである。

【０１３１】

ＳＤメモリカード２４内のメモリ領域は、普通にアクセスできるユーザデータエリアと、ドライバ（プレーヤ）２０とカード２４の間で相互認証が認められた場合にのみアクセスできるプロテクトエリアとから構成される。

【０１３２】

例えば、ＳＤメモリカードに音楽データを書き込む場合、図１０に示すように、まず、相互認証が行われる。相互認証が成功した場合には、例えば、コントローラから動作開始信号が出力され、本発明に関わる乱数シード生成回路により乱数シードが生成される。また、この乱数シードを用いて乱数が生成され、プロテクトエリアにアクセスするためのテンポラリーの鍵（セッション鍵）Ａ１が作成される。

【０１３３】

音楽データは、ドライバ（プレーヤ）２０内で鍵Ｂにより暗号化され、暗号化された音楽データがＳＤメモリカード２４内のユーザデータエリアに保存される。また、鍵Ｂは、ＳＤメモリカード２４内のプロテクトエリアに保存される。ここで鍵Ｂは、音楽データを暗号化するために使用したものであり、これが漏洩すると、音楽データの不正なコピーを発生させる危険性がある。

【０１３４】

そこで、ドライバ２０側においては、乱数を使って生成された鍵Ａ１を用いて、セキュリティ部にて鍵Ｂを暗号化し、これを、ＳＤメモリカード２４に転送する。これにより、ホストマイコンとＳＤメモリカードの間のバス情報の解析が行われないようにしている。

【０１３５】

なお、鍵Ａ１は、テンポラリーの鍵であり、プロテクトエリアにアクセスする度（又は電源投入の度）に、本発明に関わる乱数を使って作成され、かつ、プロテクトエリアにアクセスする度（又は電源投入の度）に、異なるものとなる。

【０１３６】

また、ＳＤメモリカードから音楽データを読み出す場合には、図１１に示すように、まず、相互認証が行われる。相互認証が成功した場合には、例えば、コントローラから動作開始信号が出力され、本発明に関わる乱数シード生成回路によ

り乱数シードが生成される。また、この乱数シードを用いて乱数が生成され、プロテクトエリアにアクセスするためのテンポラリーの鍵（セッション鍵）Ａ２が作成される。

【０１３７】

暗号化された音楽データは、ＳＤメモリカード２４のユーザデータエリアから読み出され、鍵Ｂは、ＳＤメモリカード２４のプロテクトエリアから読み出される。ここで、ＳＤメモリカード２４側においては、鍵Ｂを読み出すに当たって、乱数を使って生成された鍵Ａ２を用いて、セキュリティ部で鍵Ｂを暗号化し、これを、ホストマイコンに転送する。これにより、ホストマイコンとＳＤメモリカードの間のバス情報の解析が行われないようにしている。

【０１３８】

鍵Ｂは、ＳＤメモリカード２４側において、鍵Ａ２により復号される。また、この鍵Ｂを用いて、暗号化された音楽データが復号される。その結果、音楽データが再生される。

【０１３９】

なお、鍵Ａ２も、テンポラリーの鍵であり、当然に、プロテクトエリアにアクセスする度（又は電源投入の度）に、本発明に関わる乱数を使って生成され、かつ、プロテクトエリアにアクセスする度（又は電源投入の度）に、異なるものとなる。

【０１４０】

ところで、ＳＤメモリカード２４から音楽データを読み出す場合において、相互認証が失敗したときには、例えば、コントローラ（ホストマイコン）は、動作開始信号を出力しないため、本発明に関わる乱数は生成させず、結果として、テンポラリーの鍵（セッション鍵）Ａ２も、作成されない。

【０１４１】

従って、この場合、暗号化された音楽データについては読み出すことができるが、鍵Ｂを読み出すことができないため、結局、音楽データを再生することができず、音楽データの不正な読み出し又は不正なコピーが防止される。

【０１４２】

図１２は、本発明の乱数シード生成回路を有するドライバとＳＤメモリカードからなるシステムの具体例を示している。

【０１４３】

２３は、デジタル信号処理回路（ＤＳＰ）であり、乱数生成回路１１と、本発明に関わる乱数シード生成回路１３とを有している。乱数シード生成回路１３は、上述の第１乃至第８実施の形態に関わる乱数シード生成回路のいずれか１つに相当する。

【０１４４】

インターフェイス回路２２は、ＳＤメモリカード２４とデータのやりとりを行うための回路である。インターフェイス回路２２は、例えば、２０メガＨｚ程度の動作クロックで制御される。この動作クロックは、例えば、上述の第７及び第８実施の形態に関わる乱数シード生成回路を採用する場合、乱数シード生成回路内の発振器で生成される。

【０１４５】

パワーオンリセット回路１０は、ＬＳＩで使用する電源電位が安定した後に、リセット信号を出力する。このリセット信号は、コントローラ（ホストマイコン）２１に供給されると共に、上述の第１及び第２実施の形態に関わる乱数シード生成回路の場合には、デジタル信号処理回路２３にも供給される。

【０１４６】

また、上述の第３乃至第６実施の形態に関わる乱数シード生成回路の場合には、コントローラ２１は、パワーオンリセット回路１０からリセット信号を受けたときに、乱数シード生成回路１３に対して動作開始信号を出力する。また、コントローラ２１は、機器利用者の操作タイミング（例えば、再生ボタンを押したタイミングや、ＳＤメモリカードをドライバに挿入したタイミングなど）に合わせて、動作開始信号を出力してもよい。

【０１４７】

なお、このシステムにおいて、例えば、インターフェイス回路２２とデジタル信号処理回路２３は、１チップ内に形成される。また、コントローラ（ＣＰＵ）２１、インターフェイス回路２２及びデジタル信号処理回路２３を、１チップ化

しても構わない。

【０１４８】

【発明の効果】

以上、説明したように、本発明の乱数シード生成回路によれば、次のような効果を奏することができる。

【０１４９】

① 不揮発性メモリを必要とすることなく、高速クロックを発生する発振器とこれよりも遅い取り込み信号（動作開始信号）とを用いることにより、電源投入の度に、乱数シードをランダムに変えることができる。

【０１５０】

② 取り込み信号としては、パワーオンリセット回路の出力信号又はコントローラからの動作開始信号を用いることができ、簡易な構成により、乱数シードをランダムに変えることができる。

【０１５１】

③ 機器利用者の操作タイミングを利用して、乱数シード生成回路を動作させることにより、電源投入の度に、乱数シードを確実に変えることができる。

【０１５２】

④ 乱数シード生成回路により乱数シードを決定した後には、発振器を停止状態にすることにより、ＬＳＩの消費電力を小さくすることができる。

【０１５３】

⑤ 乱数シード生成回路内の発振器をＶＣＯとし、その出力クロックをシステムの動作クロックとして使用する場合に、電源を投入してから乱数シードが決定されるまでは、ＬＳＩ外部からこの発振器を制御できないようにすることで、悪意をもってＬＳＩの動作を解析することを防止できる。

【図面の簡単な説明】

【図１】

本発明の第１実施の形態に関わる乱数シード生成回路を示す図。

【図２】

図１の乱数シード生成回路の動作を示す波形図。

【図３】

本発明の第２実施の形態に関わる乱数シード生成回路を示す図。

【図４】

本発明の第３実施の形態に関わる乱数シード生成回路を示す図。

【図５】

本発明の第４実施の形態に関わる乱数シード生成回路を示す図。

【図６】

本発明の第５実施の形態に関わる乱数シード生成回路を示す図。

【図７】

本発明の第６実施の形態に関わる乱数シード生成回路を示す図。

【図８】

本発明の第７実施の形態に関わる乱数シード生成回路を示す図。

【図９】

本発明の第８実施の形態に関わる乱数シード生成回路を示す図。

【図１０】

ＳＤメモリカードを使用したシステムの概要を示す図。

【図１１】

ＳＤメモリカードを使用したシステムの概要を示す図。

【図１２】

ＳＤメモリカードとそのドライバからなるシステムを示す図。

【図１３】

従来の乱数生成回路の一例を示す図。

【図１４】

従来の乱数生成回路の一例を示す図。

【図１５】

従来の乱数を使用したシステムの一例を示す図。

【符号の説明】

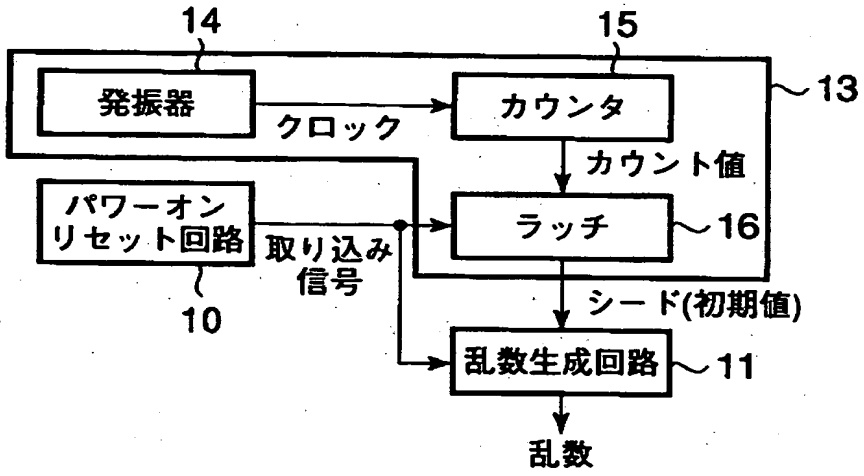
１１　　：乱数生成回路、

１２　　：不揮発性メモリ、

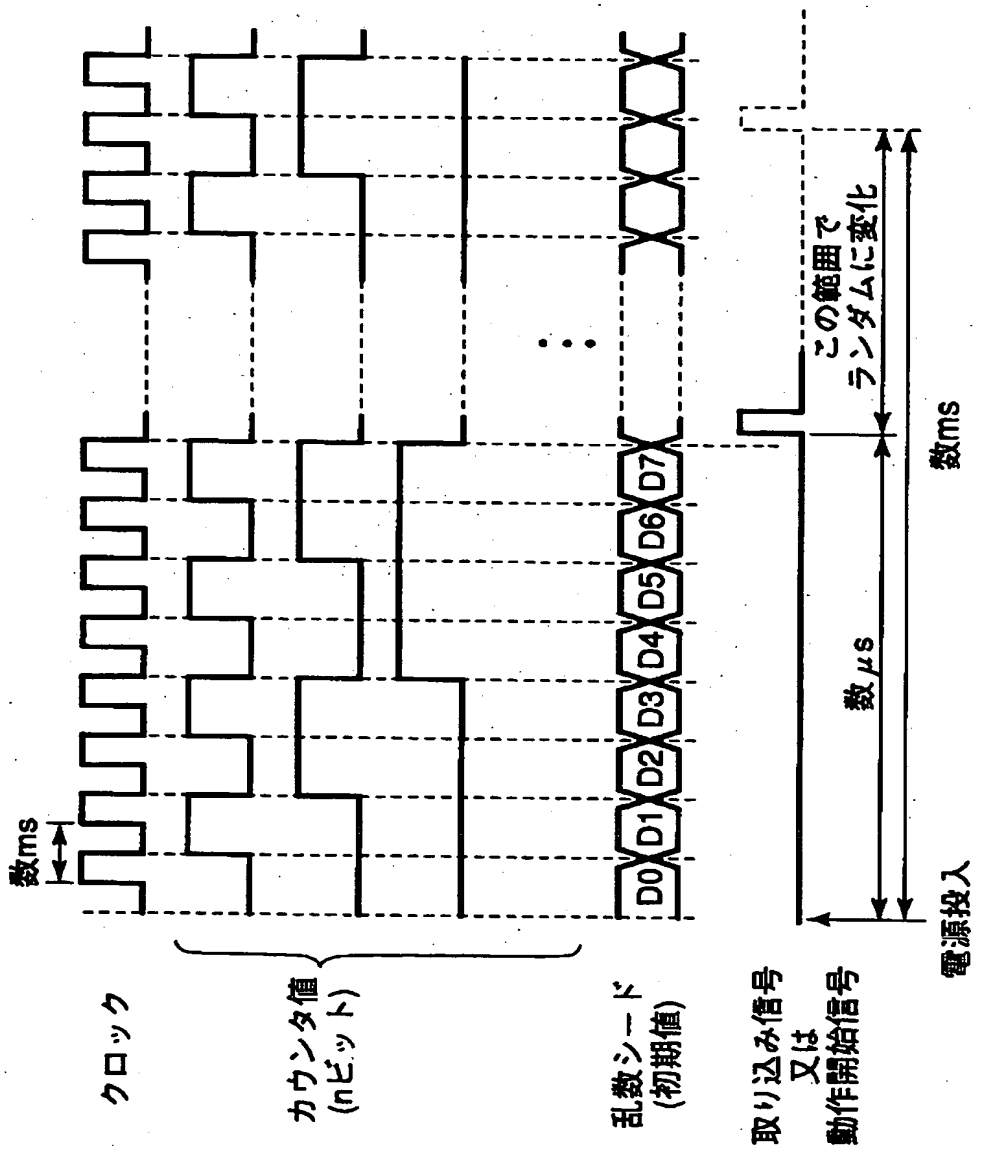
１３　：乱数シード生成回路、
１４　：発振器、
１４Ａ　：電圧制御可能な発振器（ＶＣＯ）、
１５　：カウンタ、
１６　：ラッチ回路、
１７Ａ，１７Ｂ　：分周器、
１８　：位相比較器、
１９　：ローパスフィルタ（ＬＰＦ）、
２０　：ドライバ（プレーヤ）、
２１　：コントローラ、
２２　：インターフェイス回路、
２３　：デジタル信号処理回路、
２４　：スイッチ回路。

【書類名】　図面

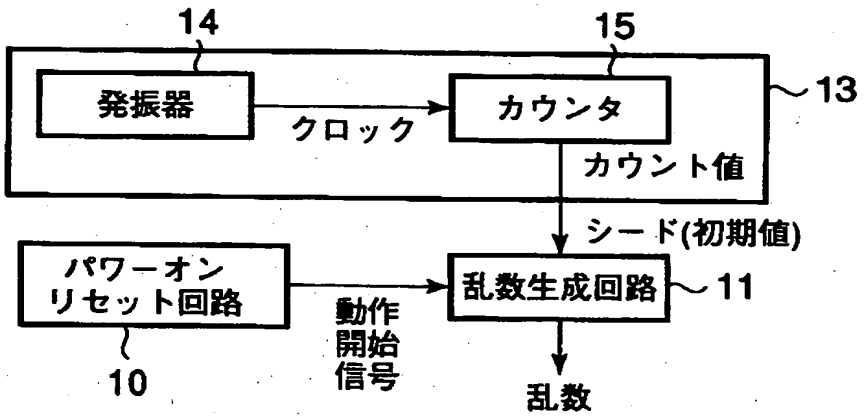
【図１】


14
15
13
発振器
クロック
カウンタ
カウント値
パワーオン
リセット回路
取り込み
信号
ラッチ
16
シード(初期値)
10
乱数生成回路
11
乱数

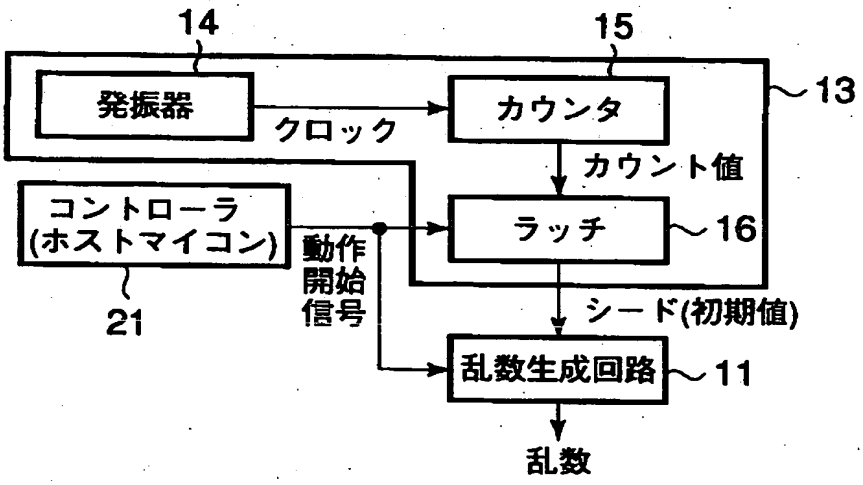
【図２】


数ms
クロック
カウンタ値
(nビット)
乱数シード
(初期値)
D0
D1
D2
D3
D4
D5
D6
D7
取り込み信号
又は
動作開始信号
この範囲で
ランダムに変化
数μs
数ms
電源投入

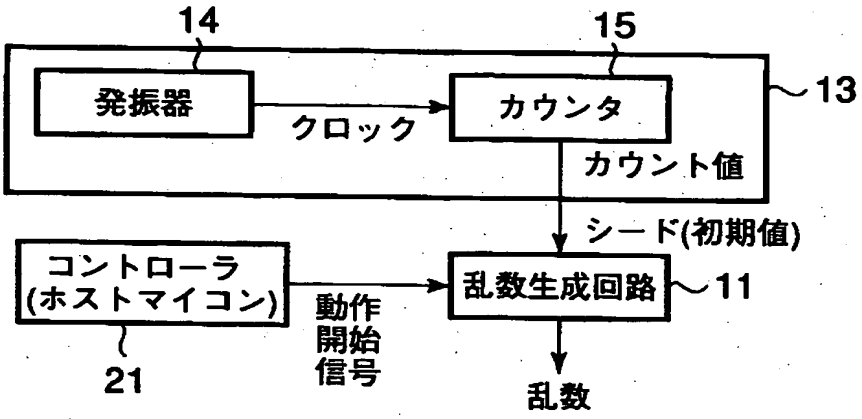
【図３】


14
15
発振器
クロック
カウンタ
13
カウント値
シード(初期値)
パワーオン
リセット回路
乱数生成回路
11
動作
開始
信号
10
乱数

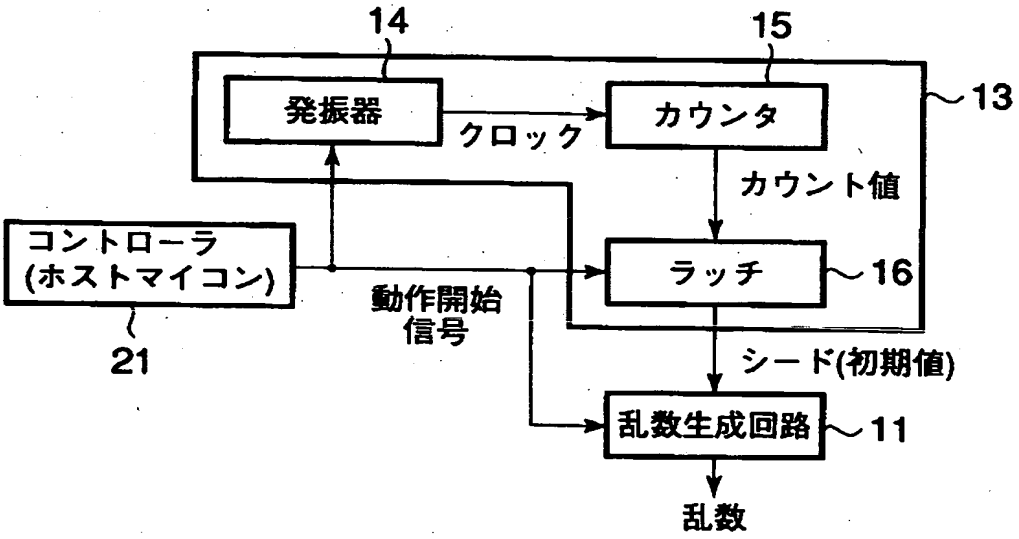
【図４】


14
15
発振器
クロック
カウンタ
13
カウント値
コントローラ
(ホストマイコン)
ラッチ
16
動作
開始
信号
21
シード(初期値)
乱数生成回路
11
乱数

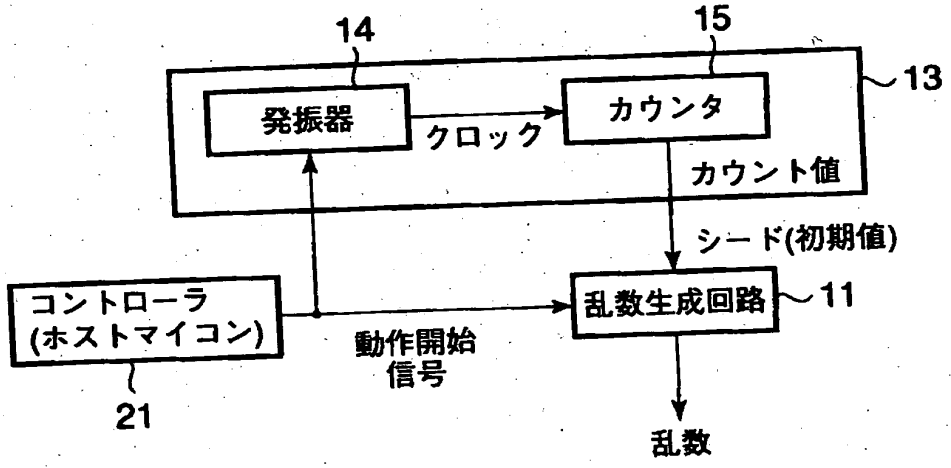
【図５】


14
15
発振器
クロック
カウンタ
13
カウント値
シード(初期値)
コントローラ
(ホストマイコン)
21
動作
開始
信号
乱数生成回路
11
乱数

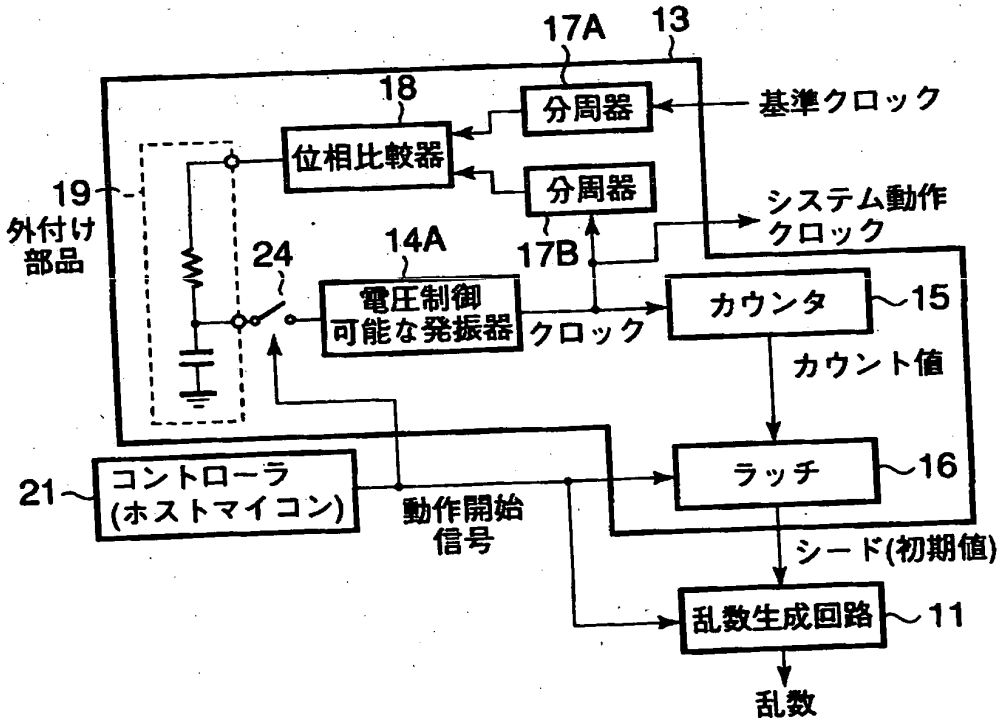
【図６】


14
15
発振器
クロック
カウンタ
13
カウント値
コントローラ
(ホストマイコン)
21
動作開始
信号
ラッチ
16
シード(初期値)
乱数生成回路
11
乱数

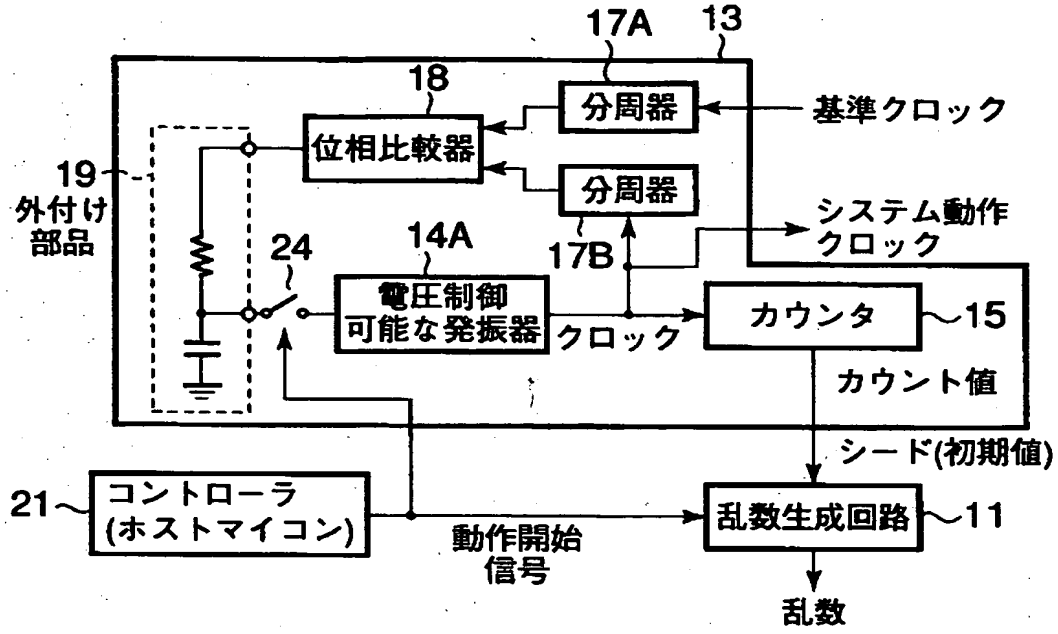
【図７】


14
15
13
発振器
クロック
カウンタ
カウント値
シード(初期値)
コントローラ
(ホストマイコン)
乱数生成回路
11
動作開始
信号
21
乱数

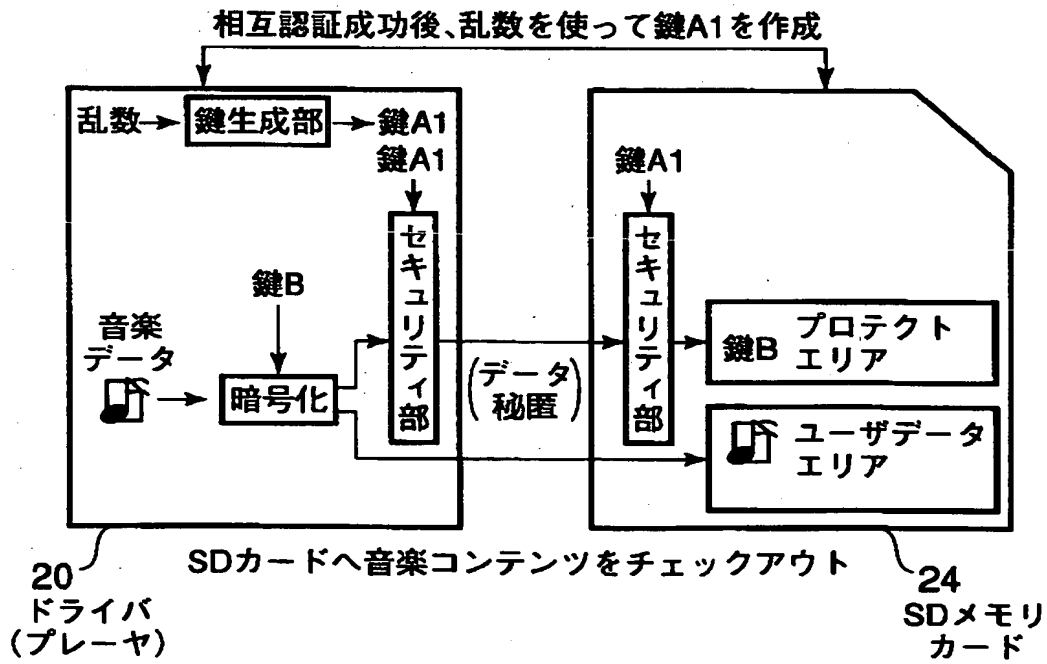
【図８】


17A
13
18
分周器
基準クロック
位相比較器
分周器
19
外付け
部品
システム動作
クロック
24
14A
17B
電圧制御
可能な発振器
クロック
カウンタ
15
カウント値
21
コントローラ
(ホストマイコン)
動作開始
信号
ラッチ
16
シード(初期値)
乱数生成回路
11
乱数

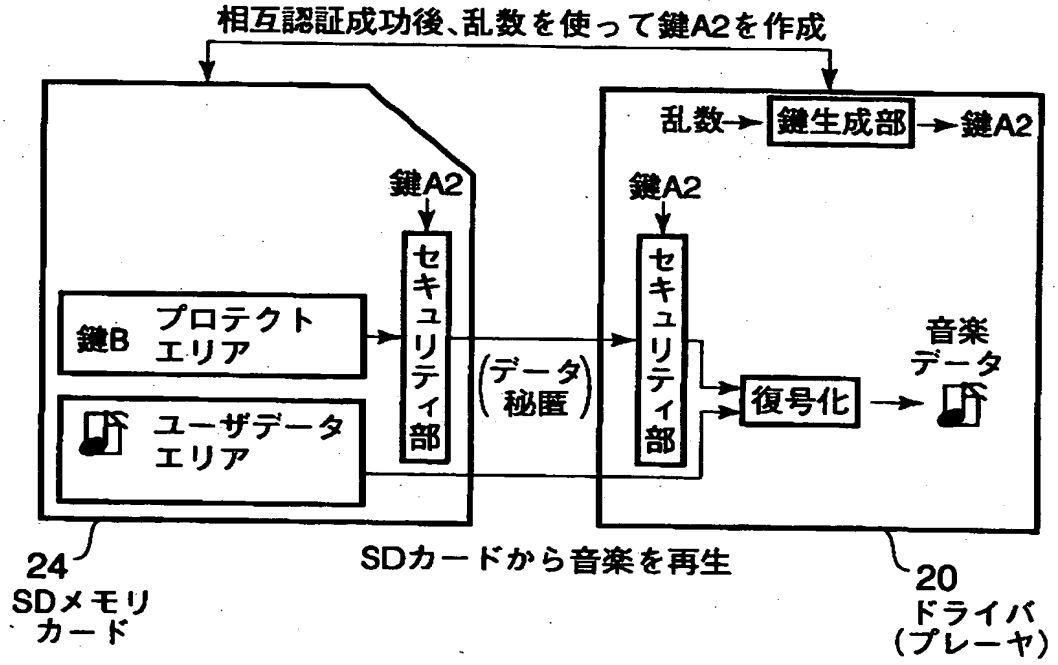
【図９】


17A
13
18
分周器
基準クロック
位相比較器
19
外付け
部品
分周器
システム動作
クロック
24
14A
17B
電圧制御
可能な発振器
クロック
カウンタ
15
カウント値
シード(初期値)
21
コントローラ
(ホストマイコン)
動作開始
信号
乱数生成回路
11
乱数

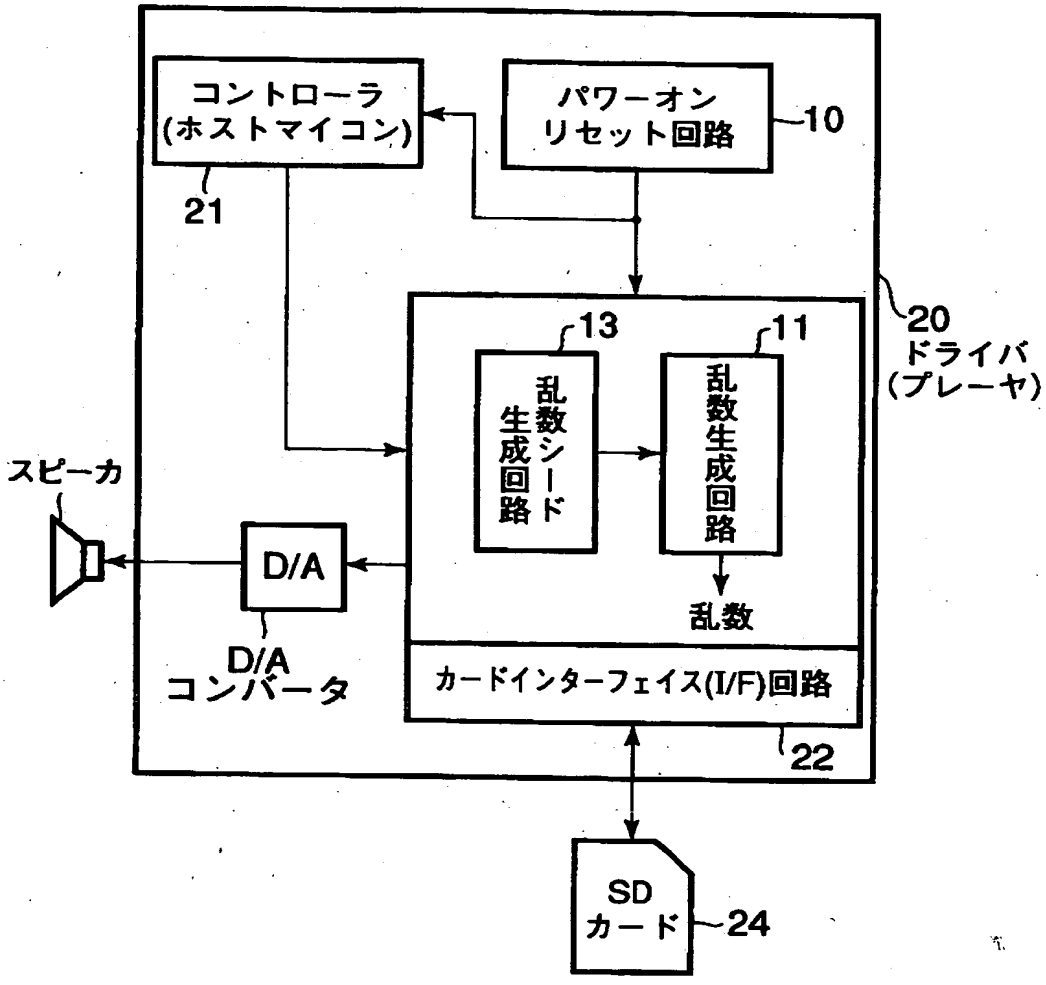
【図１０】


相互認証成功後、乱数を使って鍵A1を作成
乱数
鍵生成部
鍵A1
鍵A1
鍵A1
セキュリティ部
鍵B
音楽
データ
暗号化
(データ)
秘匿
セキュリティ部
鍵B
プロテクト
エリア
ユーザデータ
エリア
SDカードへ音楽コンテンツをチェックアウト
20
ドライバ
(プレーヤ)
24
SDメモリ
カード

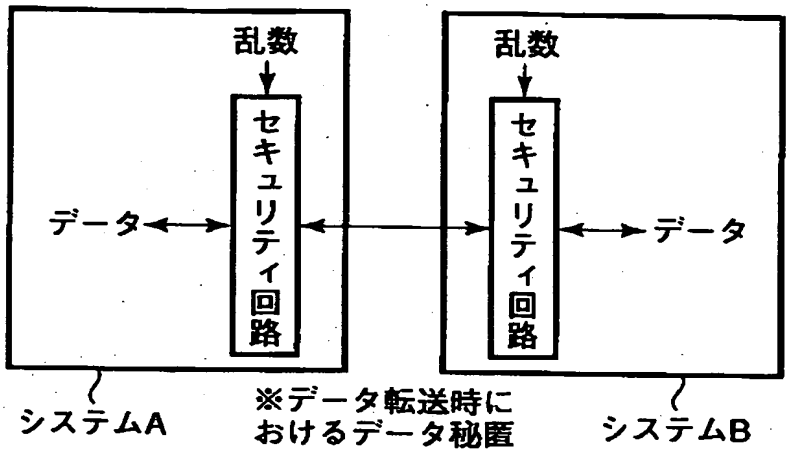
【図１１】


相互認証成功後、乱数を使って鍵A2を作成
乱数
鍵生成部
鍵A2
鍵A2
鍵A2
鍵B
プロテクト
エリア
ユーザデータ
エリア
セキュリティ部
(データ
秘匿)
セキュリティ部
復号化
音楽
データ
24
SDメモリ
カード
SDカードから音楽を再生
20
ドライバ
(プレーヤ)

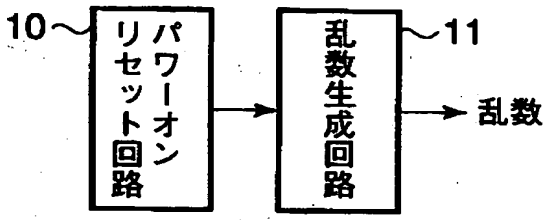
【図１２】


コントローラ
(ホストマイコン)
21
パワーオン
リセット回路
10
20
ドライバ
(プレーヤ)
13
乱数シード
生成回路
11
乱数
生成回路
乱数
スピーカ
D/A
D/A
コンバータ
カードインターフェイス(I/F)回路
22
SD
カード
24

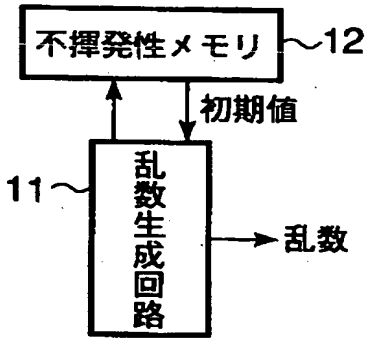
【図１３】


乱数
セキュリティ回路
データ
乱数
セキュリティ回路
データ
システムA
※データ転送時におけるデータ秘匿
システムB

【図１４】


10
パワーオンリセット回路
乱数生成回路
11
乱数

【図１５】


不揮発性メモリ
12
初期値
11
乱数生成回路
乱数

【書類名】　　要約書

【要約】

【課題】　不揮発性メモリなしに、起動の度に、乱数シードを変化させる。

【解決手段】　発振器１４は、電源投入直後から動作し、高速クロックを発生する。カウンタ１５は、この高速クロックにより動作し、カウント値を高速に変える。一方、電源が投入されてから十分な時間が経過した後、パワーオンリセット回路１０は、内部電源が安定したことを示すパワーオンリセット信号を出力する。パワーオンリセット信号は、高速クロックよりも十分に遅く、また、ラッチ回路１６に入力される時期も、まちまちとなるため、ラッチ回路１６にラッチされるカウント値（乱数シード）は、電源が投入される度に異なるものとなる。この乱数シードを用いて、乱数が生成される。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　１９９０年　８月２２日
［変更理由］　新規登録
住　所　神奈川県川崎市幸区堀川町７２番地
氏　名　株式会社東芝

２．変更年月日　　２００１年　７月　２日
［変更理由］　住所変更
住　所　東京都港区芝浦一丁目１番１号
氏　名　株式会社東芝